Amendment to the Claims:

In compliance with the Revised Amendment Format, a complete listing of claims is provided herein.

1-15. (Canceled)

16. (Currently Amended) A method of controlling card holder verification, said method comprising:

checking the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the checking comprises ~~comparing an~~ comparing by one of the card and the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device; and

if the checking indicates the presence of the trusted association, then performing card holder verification separate from the comparing using the card and without involving a holder of the card by providing another identifier to the card from the at least one device for comparing by the card to a second identifier stored on the card that is different from the first identifier, otherwise, if the checking indicates no trusted association, then involving the holder of the card in performing card holder verification by the card.

17. (Previously Presented) The method of claim 16, wherein the at least one device is located in a trusted environment.

18. (Previously Presented) The method of claim 16, wherein the card comprises a chipcard.

19. (Previously Presented) The method of claim 16, wherein the performing card holder verification without involving a holder of the card comprises performing card holder verification hidden from the holder of the card.

20. (Previously Presented) The method of claim 19, wherein the performing card holder verification hidden from the holder of the card comprises automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without intervention of the holder of the card.

21. (Canceled).

22. (Previously Presented) The method of claim 16, wherein the comparing comprises comparing a card identifier stored on the card with one or more card identifiers stored in the device.

23. (Previously Presented) The method of claim 22, wherein the card identifier is associated with a personal identification number usable in card holder verification, and said method further comprises replacing the personal identification number with another personal identification number.

24. (Previously Presented) The method of claim 22, wherein the card identifier is associated with a personal identification number usable in card holder verification, and said method further comprises erasing the association between the card identifier and the personal identification number.

25. (Previously Presented) The method of claim 16, wherein the comparing comprises comparing an identifier of the device with one or more device identifiers stored on the card.

26. (Previously Presented) The method of claim 25, wherein the device identifier is associated with a personal identification number usable in card holder verification, and said method further comprises replacing the personal identification number with another personal identification number.

27. (Previously Presented) The method of claim 25, wherein the device identifier is associated with a personal identification number usable in card holder verification, and said

method further comprises erasing the association between the device identifier and the personal identification number.

28. (Previously Presented) The method of claim 16, wherein the performing card holder verification without involving a holder of the card comprises automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without requesting information from the holder of the card, and wherein the involving the holder of the card comprises requesting the holder of the card to enter the personal identification number.

29. (Previously Presented) The method of claim 16, further comprising associating the at least one device and the card.

30. (Previously Presented) The method of claim 29, further comprising controlling the association between a device of the at least one device and the card.

31. (Previously Presented) The method of claim 30, wherein the controlling comprises using a network connectable to the device.

32. (Previously Presented) The method of claim 16, wherein the checking is between at least one device and a plurality of cards, and wherein the performing card holder verification without involving a holder of the card is for a plurality of holders.

33. (Currently Amended) A method of performing card holder verification, said method comprising:

checking the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the checking comprises comparing by one of the card and the at least one device a first ~~comparing an~~ identifier stored on the card with one or more identifiers stored in the at least one device; and

performing card holder verification by the card separate from and based on the checking, wherein:

if the checking indicates the presence of the trusted association, then a personal identification number of the holder of the card different from the first identifier is automatically ~~obtained~~ provided to the card from the at least one device, and verified using the card without requesting information from the holder of the card;

however, if the checking indicates no trusted association, then the holder of the card is requested to enter the personal identification number to verify the holder of the card via the card comparing the personal identification number entered to a second identifier stored on the card.

34. (Currently Amended) A system of controlling card holder verification, said system comprising:

means for checking the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the means for checking comprises means for comparing by one of the card and the at least one device a first ~~comparing an~~ identifier stored on the card with one or more identifiers stored in the at least one device; and

means for performing card holder verification separate from the comparing using the card and without involving a holder of the card by providing another identifier to the card from the at least one device for comparing by the card to a second identifier stored

on the card that is different from the first identifier, if the checking indicates the presence of the trusted association, ~~or for~~ and means for involving the holder of the card in performing card holder verification by the card, if the checking indicates no trusted association.

35. (Previously Presented) The system of claim 34, wherein the means for performing card holder verification without involving a holder of the card comprises means for performing card holder verification hidden from the holder of the card.

36. (Previously Presented) The system of claim 35, wherein the means for performing card holder verification hidden from the holder of the card comprises means for automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without intervention of the holder of the card.

37. (Canceled).

38. (Previously Presented) The system of claim 34, wherein the means for comparing comprises means for comparing a card identifier stored on the card with one or more card identifiers stored in the device.

39. (Previously Presented) The system of claim 34, wherein the means for comparing comprises means for comparing an identifier of the device with one or more device identifiers stored on the card.

40. (Currently Amended) A system of performing card holder verification, said system comprising:

at least one processor on the card to perform card holder verification based on whether a trusted association exists between at least one device and a card usable with the at least one device, and to ~~compare an~~ compare a first identifier stored on the card with one or more identifiers stored in the at least one device, wherein:

if a checking of the trusted association indicates the presence of the trusted association, then a personal identification number different from the first identifier of the holder of the card is automatically ~~obtained~~ provided to the card from the at least one device, and verified separate from the compare using the card without requesting information from the holder of the card;

however, if the checking indicates no trusted association, then the holder of the card is requested to enter the personal identification number to verify the holder of the card via the card comparing the personal identification number to a second identifier stored on the card.

41. (Currently Amended) An article of manufacture comprising:

at least one computer usable medium having computer readable program code logic to control card holder verification, the computer readable program code logic comprising:

check logic to check the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the check logic comprises compare logic to ~~compare an~~ compare by one of the card and the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device; and

logic to perform card holder verification separate from the compare using the card and without involving a holder of the card by providing another identifier to the card from the at least one device for comparing by the card to a second identifier stored on the card that is different from the first identifier, if the checking indicates the presence of the trusted association, ~~or to~~ and logic to involve the holder of the card in performing card holder verification by the card, if the checking indicates no trusted association.

42. (Previously Presented) The article of manufacture of claim 41, wherein the logic to perform card holder verification without involving a holder of the card comprises perform logic to perform card holder verification hidden from the holder of the card.

43. (Previously Presented) The article of manufacture of claim 42, wherein the perform logic comprises obtain logic to automatically obtain a personal identification number of the holder of the card and verify logic to verify the personal identification number without intervention of the holder of the card.

44. (Canceled).

45. (Previously Presented) The article of manufacture of claim 41, wherein the compare logic comprises compare logic to compare a card identifier stored on the card with one or more card identifiers stored in the device.

46. (Previously Presented) The article of manufacture of claim 41, wherein the compare logic comprises compare logic to compare an identifier of the device with one or more device identifiers stored on the card.

47. (Currently Amended) An article of manufacture comprising:

at least one computer usable medium having computer readable program code logic to perform card holder verification, the computer readable program code logic comprising:

check logic to check the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the check logic comprises compare logic to ~~compare an~~ compare by one of the card and the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device; and

perform logic to perform card holder verification by the card based on the checking, wherein:

if the checking indicates the presence of the trusted association, then a personal identification number of the holder of the card different from the first identifier is automatically ~~obtained~~ provided to the card from the at least one device, and verified separate from the compare using the card and without requesting information from the holder of the card;

however, if the checking indicates no trusted association, then the holder of the card is requested to enter the personal identification number to verify the holder of the card via the card comparing the personal identification number entered to a second identifier stored on the card.